Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

Vyhláška o nepominutelných funkcích stanoveného rozsahu

A. Obecná část

a) Vysvětlení nezbytnosti navrhované právní úpravy, odůvodnění jejích hlavních principů

V navrhovaném zákoně o kybernetické bezpečnosti (dále též „Zákon“) zahrnujícím mechanismus prověřování bezpečnosti dodavatelského řetězce (dále jen „mechanismus posuzování dodavatelů), dochází k zavedení pojmu „kritická část stanoveného rozsahu“ v § X *[Prověřování rizik spojených s dodavatelem]*. Tím se pro potřeby mechanismu posuzování dodavatelů rozumí aktiva stanoveného rozsahu zajišťující nepominutelné funkce nebo aktiva stanoveného rozsahu, u kterých byl poskytovatel regulované služby v režimu vyšších povinností, na kterého dopadají povinnosti z mechanismu posuzování dodavatelů ohodnocen dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká či kritická (dále jen „vysoká či kritická aktiva“).

Zákon tak stanovuje dva způsoby určení kritické části stanoveného rozsahu, přičemž tyto lze rozdělit na subjektivní (závislé na vůli poskytovatele regulované služby) a objektivní (nezávislé na vůli poskytovatele regulované služby).

Prostřednictvím samoidentifikace může poskytovatel regulované služby v režimu vyšších povinností u aktiv stanoveného rozsahu, postupem dle vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, ohodnotit dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká či kritická. Tím se stanou kritickou součástí stanoveného rozsahu.

Druhým způsobem je určení kritické části stanoveného rozsahu ve spojitosti s nepominutelnými funkcemi stanovenými v podzákonném právním předpise. Pokud aktiva stanoveného rozsahu zajišťují takto stanovené nepominutelné funkce, jedná se o kritickou součást stanoveného rozsahu. Zákon zmocňuje v § X *[Prováděcí právní předpisy a zmocňovací ustanovení]* Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vydat prováděcí právní předpis, ve kterém nepominutelné funkce stanoví.

Tato vyhláška je odrazem druhého ze shora uvedených způsobů. Jejím účelem je stanovit a konkretizovat nepominutelné funkce, aby byla objektivně stanovena množina aktiv, které jsou natolik kritické, že dodavatelé plnění do těchto funkcí musí podléhat mechanismu posuzování dodavatelů.

Vzhledem k dynamickému vývoji moderních technologií a potřebě kvalifikovaného stanovení nepominutelných funkcí je třeba velmi pečlivě a s rozvahou identifikovat, jaké funkce budou do této množiny spadat. Byť vůlí zákonodárce je vymezit veškeré tyto funkce v rámci jednoho prováděcího právního předpisu, je zřejmé, že identifikace všech kritických funkcí, jež by měly být identifikovány jako nepominutelné, je časově a kapacitně velmi náročné a vyžaduje značnou odbornost. Vydání takto celistvé vyhlášky ihned při přijetí Zákona či krátce poté, nelze reálně očekávat.

Současně je ale zřejmé, že bez dostatečně rychlého vydání podzákonného právního předpisu, který by stanovil nepominutelné funkce, bude aktivace mechanismu posuzování dodavatelů odvislá pouze od subjektivního způsobu určení kritické části stanoveného rozsahu, jak byl shora stručně uveden. Takový stav by byl dlouhodobě velmi neuspokojivý, jelikož by

mohlo docházet k rozdílným přístupům i kvalitě provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb. Jako vysoká či kritická by nemusela být ohodnocena všechna aktiva, na nichž bude poskytování regulované služby vždy vysoce závislé. Tím by docházelo i k rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli vztahujícímu se k takovým aktivům. Tento stav by nebyl v souladu s bezpečnostními zájmy státu.

S ohledem na velmi závažný dopad mechanismu posuzování dodavatelů je proto nezbytné, aby NÚKIB nepominutelné funkce jednotlivých regulovaných systémů určoval, není-li o kritičnosti či vysoké důležitosti aktiv, která tyto funkce zajišťují, pro poskytování regulované služby pochyb. Cílem NÚKIB není určení všech funkcí, které jsou zajišťovány vysokými a kritickými aktivy u jednotlivých systémů či sektorů, nicméně vymezení takových funkcí, jejichž významnost je nezpochybnitelná a jež jsou zajištěny prostřednictvím aktiv, která by měla být vždy ohodnocena jako vysoká či kritická, protože na nich bude poskytování regulované služby vždy vysoce závislé.

Oblastí, na kterou dopadá navrhovaný rozsah vyhlášky, je sektor elektronických komunikací, s jehož charakteristickými rysy má NÚKIB za dobu své existence značné zkušenosti. Současně se jedná o technologickou oblast, pro kterou má ICT klíčový význam a která je vnitrostátně i mezinárodně vysoce standardizovaná. V České republice je tato oblast rovněž specificky regulována v rámci zákona č. 127/2005 Sb., zákon o elektronických komunikacích a o změně některých souvisejících zákonů, v jehož rámci je zřízen Český telekomunikační úřad, který na dodržování regulace dohlíží. Stát má proto dostatečné kapacity, aby mohl odpovědným způsobem autoritativně určit nepominutelné funkce elektronických komunikací, a to včetně dosud plně nezavedených sítí 5. generace.

K obdobnému vymezení tzv. kritických funkcí pro sektor elektronických komunikací přistoupilo i mnoho dalších států (jako např. Spojené království), vč. států Evropské unie (Francie, Německo či Finsko). Přehled kritických funkcí sítí elektronických komunikací zveřejnila jako součást Souboru opatření EU pro kybernetickou bezpečnost sítí 5G (dále jen „EU 5G Toolbox“) také Skupina pro spolupráci (tzv. NIS Cooperation Group).

EU 5G Toolbox[1] označuje za kritické funkce 5G sítí funkce spojené s jádrem sítě (tzv. core network functions), funkce správy a síťové orchestrace (dále také „MANO“). Za vysoce důležitou funkci je považována funkce přístupu k radiové síti (dále také „RAN“). Za středně či vysoce důležité jsou dále považovány funkce ostatních systémů řízení a podpůrných služeb kromě MANO, transportní a přenosové funkce a funkce internetwork exchanges.

Obdobně k hodnocení kritičnosti funkcí 5G sítí přistupuje také německý regulátor sektoru elektronických komunikací Bundesnetzagentur (dále také „BNetzA“). BNetzA do seznamu kritických funkcí[2] zařadil všechny funkce popsané v EU 5G Toolboxu, tedy funkce spojené s jádrem sítě, funkce MANO, funkce ostatních systémů řízení a podpůrných služeb, transportní a přenosové funkce a funkce internetwork exchanges.

Také Národní centrum kybernetické bezpečnosti Spojeného království (dále jen „NCSC“) vydalo doporučení pro vymezení rozsahu sítí 5G, 4G i sítí elektronických komunikací obecně. Toto vymezení specifikuje části sítí, kde přítomnost tzv. vysoce rizikového dodavatele[3] nelze mitigovat technickými opatřeními. Jedná se o vymezení částí sítí elektronických komunikací, kde by zařízení vysoce rizikových dodavatelů neměla být vůbec využívána. Toto vymezení

[1] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468, str. 29-40.

[2] Katalog der Sicherheitsanforderungen (bundesnetzagentur.de), str. 4.

[3] Vysoce rizikový dodavatel z pohledu NCSC je specifikován v Doporučení NCSC pro využívání zařízení vysoce rizikových dodavatelů v telekomunikačních sítích Spojeného království. Dostupné zde: NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK

funkcí je poměrně podrobně popsáno v Doporučení NCSC pro využívání zařízení vysoce rizikových dodavatelů v telekomunikačních sítích Spojeného království.[4]

Francie v Kodexu poštovní a elektronické komunikace (Code des postes et des communications électroniques)[5] specifikuje zařízení, resp. funkce 5G sítí, jejichž pořízení podléhá udělení povolení ze strany státu. V případě francouzské regulace se jedná o specifikaci funkcí dle standardů 3GPP pro 5G sítě, konkrétně do této kategorie spadají funkce New Radio Base Station (en-gNodeB a gNodeB), Access and Mobility management Function (AMF), Authentication Server Function (AUSF), User Plane Function (UPF), Session Management Function (SMF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), Network Repository Function (NRF), Network Exposure Function (NEF), Unified Data Management (UDM) a Security Edge Protection Proxy (SEPP).

Velmi podrobně vymezené kritické části sítě elektronických komunikací má také Finsko. Finská dopravní a komunikační agentura TRAFICOM vymezuje zejména kritické funkce 4G sítě, 5G sítě i sítě elektronických komunikací obecně.[6] Do tohoto výčtu zahrnuje úžeji vymezené funkce než např. Německo či Skupina pro spolupráci v EU 5G Toolboxu.

Návrh vyhlášky předkládá NÚKIB na základě zmocnění uvedeného v § X zákona o kybernetické bezpečnosti, k provedení obsahu ustanovení § X tohoto zákona.

b) Zhodnocení souladu návrhu vyhlášky s ústavním pořádkem České republiky a se zákonem, k jehož provedení se navrhuje

Návrh vyhlášky je v souladu s ústavním pořádkem České republiky.

Jako prováděcí právní předpis odráží soulad Zákona s ústavním pořádkem. Navrhovaná právní regulace kybernetické bezpečnosti se dotýká především práva vlastnického a částečně též i z něj odvozovaného práva na svobodu podnikání dle Listiny základních práv a svobod. Povinnosti, které navrhovaná právní úprava stanoví vybraným subjektům (tzv. poskytovatelům regulované služby), totiž v různé míře omezují tyto subjekty v možnosti neomezeně užívat systémy, k nimž vykonávají vlastnická nebo obdobná práva.

Zákonná právní úprava v rámci těchto práv omezuje povinné subjekty v zásadě plošně. Plošné omezení vlastnického práva, resp. práva na podnikání, má v tomto případě formu zavedení povinností, zejména implementovat bezpečnostní opatření, hlásit kybernetické bezpečnostní incidenty a provádět vydaná protiopatření. Úzké části poskytovatelů regulované služby s potenciálně největšími dopady pro fungování České republiky může také omezit vlastnické právo, resp. právo na podnikání, v rámci nově zaváděného mechanismu posuzování dodavatelů.

Zákon, na který obsahově navazuje tento návrh vyhlášky, se vypořádal s odůvodněním narušení výše uvedených práv následovně. S ohledem jak na zájmy bezpečnostní, tak i ekonomické, je stanovení nepominutelných funkcí orientováno na minimalistický přístup, jehož podstatou je podřadit pod regulaci návrhu zákona prvky vyžadující ochranu, nicméně nepřekračovat a neregulovat subjekty v České republice plošně.

Možné omezení práva na užívání majetku, za které by snad povinná bezpečnostní opatření uložená tímto Zákonem a jeho budoucími prováděcími předpisy mohla být považována, má za účel chránit obecné zájmy, kterými je bezpečnost státu a obyvatelstva či

[4] NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK

[5] Arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et des communications électroniques - Légifrance (legifrance.gouv.fr)

[6] Regulation on critical parts of a communications network

významné ekonomické a společenské zájmy. Kybernetická bezpečnost České republiky jako podmnožina bezpečnosti České republiky spadá do rozsahu působnosti ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. Podle čl. 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot základní povinností státu. Návrh zákona lze považovat za jeden z prostředků plnění této povinnosti státu. Návrh zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž Česká republika jako členský stát Evropské unie usiluje.

Návrh vyhlášky je rovněž v souladu s obsahem zákona o kybernetické bezpečnosti, k jehož provedení se navrhuje, protože reflektuje mantinely stanovené zmocňovacím ustavením tohoto zákona a nepřekračuje je. Dle zákona má prováděcí právní předpis stanovit toliko množinu konkrétních nepominutelných funkcí, které jsou zajišťovány kritickými či vysokými aktivy.

c) Zhodnocení souladu návrhu vyhlášky s mezinárodními smlouvami, jimiž je Česká republika vázána, judikaturou ESLP a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

V oblasti kybernetické bezpečnosti nebyla dosud uzavřena žádná mezinárodní smlouva. Druhotně se kybernetické bezpečnosti dotýká Úmluva Rady Evropy o kyberkriminalitě, rovněž známá jako Budapešťská úmluva. Zákon o kybernetické bezpečnosti a jeho prováděcí předpisy včetně tohoto návrhu vyhlášky jdou rovněž v duchu nezávazných doporučení a závazků chránit důležité informační systémy formulovaných například ve zprávách Skupiny expertů OSN (UN GGE) či v opatřeních pro budování důvěry přijatých účastnickými státy Organizace pro bezpečnost a spolupráci v Evropě.

Přímo se kybernetické bezpečnosti nedotýká ani judikatura Evropského soudu pro lidská práva. Problematiku související s návrhem právního předpisu lze posuzovat z hlediska práv chráněných Evropskou úmluvou o lidských právech, např. práva na pokojné užívání majetku (povinné zavádění bezpečnostních opatření), práva na respektování soukromí (kompromitace citlivých údajů jako jedno z dopadových kritérií), práva na spravedlivé řízení (proces určování provozovatelů základních služeb) či práva nebýt dvakrát stíhán či trestán (správní řízení o porušení povinností podle zákona o kybernetické bezpečnosti v kontrapozici proti trestněprávní odpovědnosti). Navrhovaná úprava však nejenže nepředstavuje zásah do těchto práv či jejich nepřiměřené omezení, naopak v některých případech přispívá k jejich ochraně zajištěním adekvátní úrovně bezpečnosti informací tím, že realizuje zákonné zmocnění obsažené v zákoně o kybernetické bezpečnosti.

Znění návrhu vyhlášky vychází rovněž z přístupů k chráněným či nepominutelným funkcím dalších členských států EU. V rámci mezinárodní spolupráce provedl NÚKIB sérii bilaterálních jednání[7] určených k seznámení se s jednotlivými národními přístupy, které úřad provedl především v průběhu roku 2022.

Obsah tohoto návrhu vyhlášky nemá žádný vztah k obsahu nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013, tzv. „aktu o kybernetické bezpečnosti“.

[7] Německo, Velká Británie.

Navrhované znění vyhlášky bere také v potaz obsah směrnice Evropského parlamentu a Rady o posílení kritických subjektů (tzv. směrnice CER).

Návrh vyhlášky je v souladu s obecnými zásadami práva Evropské unie, jako jsou např. zásada právní jistoty, proporcionality a zákaz diskriminace.

Návrh vyhlášky není v rozporu s judikaturou soudních orgánů Evropské unie a je v souladu s obecnými zásadami práva Evropské unie (např. zásadou právní jistoty, proporcionality a zákazem diskriminace).

Na základě těchto skutečností je možné návrh vyhlášky hodnotit jako plně slučitelný s právem Evropské unie.

d) Předpokládaný hospodářský a finanční dosah navrhované právní úpravy na veřejné rozpočty a dopad na podnikatelské prostředí České republiky

Vymezení hospodářských a finančních dosahů navrhované právní úpravy je součástí Závěrečné zprávy RIA v důvodové zprávě zpracované k zákonu o kybernetické bezpečnosti, který tento návrh vyhlášky provádí, přičemž zahrnuje i personální a s nimi související rozpočtové otázky vyplývající z činností NÚKIB.

Zákon o kybernetické bezpečnosti tvoří především transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). Z obecných odhadů vytvořených NÚKIB vyplývá, že splněním požadavků směrnice dojde k nárůstu počtu regulovaných subjektů z nižších stovek (cca 400) podle předchozí právní úpravy na vyšší tisíce (nejméně 6000). Úprava bezpečnosti dodavatelského řetězce se však bude týkat pouze zlomku z výše uvedených regulovaných subjektů. Povinnými osobami mechanismu jsou poskytovatelé takových regulovaných služeb, které naplňují kritéria pro určení regulované služby v režimu vyšších povinností, a zároveň by narušení bezpečnosti informací poskytovatelem regulované služby mohlo způsobit závažný dopad na bezpečnost České republiky nebo vnitřní či veřejný pořádek. Jedná se o cca 150 subjektů.

Návrh vyhlášky vymezuje nepominutelné funkce dle § X odst. 3 *[Prověřování rizik spojených s dodavatelem]* zákona, jež jsou pro zajištění agendy bezpečnosti dodavatelského řetězce a určení jejího dopadu klíčové.

Je možné, že přímo v souvislosti s navrhovanou vyhláškou dojde k rozšíření kritické části stanoveného rozsahu povinných osob mechanismu v sektoru elektronických komunikací. Z toho plyne možné rozšíření počtu dodavatelů, kteří budou moci mechanismu posuzování dodavatelů podléhat a kteří budou moci být omezeni. V případě vydání varování dle zákona o kybernetické bezpečnosti se bude jednat o povinnost povinné osoby mechanismu reflektovat identifikovanou hrozbu v analýze rizik, což je proces, který je v současnosti u povinných osob mechanismu již nastavený a fungující.

Případný zákaz dodavatele má potenciální vysoký dopad na povinné osoby. Pokud by povinná osoba identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně relevantní dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit. Z dotazníkového šetření[8] plyne, že vyloučení a nahrazení významného dodavatele

[8] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby

může pro povinnou osobu mechanismu generovat náklady až ve výši[9] jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů), stovek milionů Kč (16 % respondentů). Tyto náklady spočívají ve výměně stávajícího řešení, pořízení nového řešení a jeho integraci mezi stávající infrastrukturu a procesy, přičemž vždy ale bude záležet o jakého dodavatele se jedná a jaké podmínky nabízí dodavatelé alternativní. 22 % respondentů uvedlo, že vyloučení takového dodavatele nebude mít žádný dopad. 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny na takové výše z důvodu, že dané orgány či osoby uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávali mj. dopady ukončení či omezení poskytování regulované služby, vč. ušlého zisku. Pro případ unikátnosti dodávky daného vysoce bezpečnostně rizikového dodavatele NÚKIB umožňuje v rámci procesu připomínkování návrhu opatření obecné povahy povinným osobám mechanismu tento fakt NÚKIB sdělit. V případě dostatečného odůvodnění a podložení tvrzení důkazy může NÚKIB udělit výjimku pro typovou bezpečnostně relevantní dodávku a povinným osobám mechanismu za podmínek reflektování identifikované hrozby v analýze rizik a umožnit bezpečnostně relevantní dodávku využívat i nadále, čímž jsou případné náklady plynoucí ze zákazu takového dodavatele pro povinnou osobu minimalizovány. Jelikož tedy navrhovaná právní úprava pro případy existence jediného možného dodavatele poskytujícího bezpečnostně relevantní dodávku umožňuje získat výjimku ze zákazu takového dodavatele pro danou bezpečnostně relevantní dodávku, s generováním respondenty udaných vysokých nákladů (vyšších než 1 miliardu Kč) předkladatel nepočítá.

56 % respondentů jako nejzávažnější možný dopad na poskytování služby identifikuje omezení či ukončení poskytování služby. Právě riziko ohrožení poskytování regulované služby podstatným způsobem také umožňuje poskytovateli regulované služby zažádat o výjimku ze zákazu plnění identifikovaného vysoce rizikového dodavatele. Pro dalších 32 % respondentů jsou nejzávažnější dopady finanční a 12 % respondentů v případě aplikace lhůty respektující ekonomickou životnost daného aktiva vyloučení stávajícího dodavatele identifikuje s absencí dopadů vyšších než ty, které jsou s obnovou technologie a přechodem na alternativní technologická řešení standardně spojena.

V případě, že povinná osoba vysoce rizikového dodavatele v současnosti nevyužívá, nicméně v budoucnu by o bezpečnostně relevantních dodávkách tohoto dodavatele uvažovala, z důvodu vyloučení možnosti bezpečnostně relevantní dodávku od vysoce rizikového dodavatele pořídit může docházet k obdržení vyšší ceny od alternativních dodavatelů dodávek. Tento přístup a zvýšené náklady se mohou objevit obzvláště v případě, že na trhu není dostatečná konkurence a danou dodávku poskytuje pouze omezený počet dodavatelů.

Vymezením nepominutelných funkcí by mělo dojít k zefektivnění určování a udržování kritických částí systémů regulovaných subjektů. Dále dojde k aplikaci povinností plynoucích z mechanismu posuzování dodavatelů napříč povinnými osobami mechanismu obdobným způsobem, a to zejména tím, že funkce, jejichž významnost je nezpochybnitelná, tedy takové funkce, které jsou zajištěny aktivy, která by měla být vždy ohodnocena jako vysoká či kritická, protože na nich bude poskytování regulované služby vždy vysoce závislé, budou pevně stanoveny. Dojde tak k zamezení negativních dopadů možného rozdílného přístupu i kvality

spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

[9] Na otázku uvedení maximálního finančního dopadu na zastupovanou organizaci v případě zákazu využívání plnění nejvýznamněji zastoupeného významného dodavatele dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti po uplynutí ekonomické životnosti poskytovaného aktiva obdržel NÚKIB 32 odpovědí, které lze kvantifikovat.

provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb v režimu vyšších povinností, na něž dopadá mechanismus posuzování dodavatelů.

e) Předpokládané sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel; dopady na životní prostředí

Návrh vyhlášky je z hlediska sociálních dopadů a dopadů na specifické skupiny obyvatel neutrální. Zvýšení úrovně kybernetické bezpečnosti a tím pádem zajištění regulovaných služeb bude mít druhotný pozitivní dopad na společenské a ekonomické činnosti jako např. zajištění zdravotní péče či dodávky energie. Návrh vyhlášky je rovněž neutrální z hlediska dopadů na životní prostředí, lze však obdobně předpokládat pozitivní efekt v podobě předcházení takových bezpečnostních incidentů, které by negativní dopad mohly mít.

f) Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Navrhovaná právní úprava je z hlediska zákazu diskriminace a z hlediska rovnosti mužů a žen neutrální.

g) Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů a dopadů na výkon státní statistické služby

Znění zákona o kybernetické bezpečnosti posiluje spolupráci mezi národními autoritami v oblasti kybernetické bezpečnosti i ochrany osobních údajů. Návrh vyhlášky je v ohledu ochrany osobních údajů bezrozporný, jelikož nestanoví žádné podmínky zásahu do ochrany osobních údajů. Druhotně může mít navrhovaná právní úprava pozitivní dopad na ochranu soukromí a osobních údajů, neboť rozšířením regulace v souladu s obsahem směrnice a tímto návrhem vyhlášky na nové subjekty dojde k rozšíření veřejnoprávní regulace kybernetické bezpečnosti, která může mít z pohledu zavádění přiměřených organizačních a technických opatření kladný dopad také na ochranu osobních údajů v regulovaných organizacích.

Navrhovaná úprava nebude mít dopad na výkon státní statistické služby.

h) Zhodnocení korupčních rizik

V této oblasti nebyla shledána žádná nová vazba ani nová rizika. Právě naopak, zkonkretizování nepominutelných funkcí má snahu zamezit případnému rozdílnému přístupu i kvalitě provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb, a tedy i k rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli vztahujícímu se k těmto aktivům.

Návrh právní úpravy je jednoznačný a vychází z právního rámce daného zákonem o kybernetické bezpečnosti, který doplňuje o omezený okruh povinných osob. Tomuto okruhu přiřazuje na základě dopředu stanovených kritérií režimy povinností.

i) Zhodnocení dopadů na bezpečnost nebo obranu státu

Vzhledem k povaze navrhovaných změn lze konstatovat, že návrh vyhlášky má velmi pozitivní dopady na bezpečnost a obranu státu. Určením nepominutelných funkcí se zajistí ochrana kritických částí systémů regulovaných subjektů v důsledku čehož dojde k navýšení úrovně kybernetické bezpečnosti, odolnosti strategické infrastruktury a stability služeb v České republice.

Ochrana nepominutelných funkcí může mít s ohledem na její povahu v návrhu vyhlášky pozitivní dopad na bezpečnost a obranu státu, zejména díky schopnosti centralizovat

a vyhodnocovat informace o bezpečnostních hrozbách a zranitelnostech k těmto funkcím z celého světa, a na základě toho přijímat potřebné kroky dříve a ve vyšší kvalitě.

Dále dojde k aplikaci povinností plynoucích z mechanismu posuzování dodavatelů napříč povinnými osobami mechanismu obdobným způsobem, a to zejména tím, že funkce, jejichž významnost je nezpochybnitelná a jež jsou zajišťovány aktivy, která by měla být vždy ohodnocena jako vysoká či kritická, protože na nich bude poskytování regulované služby vždy vysoce závislé, budou pevně stanovena. Dojde tak k zamezení případnému rozdílnému přístupu i kvalitě provedení identifikace vysokých a kritických aktiv jednotlivými poskytovateli regulovaných služeb, a tedy i k rozdílnému způsobu aplikace zmírňování rizik spojených s dodavateli vztahujícímu se k těmto aktivům, což bude mít pozitivní vliv na bezpečnost státu.

j) Konzultace

Podstatnou součástí procesu tvorby návrhu vyhlášky byla ze strany NÚKIB série bilaterálních jednání, zaměřená především na oslovení zástupců státních orgánů spolupracujících na přípravě Zákona, regulátora sektoru elektronických komunikací Českého telekomunikačního úřadu, dalších relevantních organizací a subjektů v rámci budoucích regulovaných odvětví, a vlastní šetření spočívající ve zkoumání a komparaci jednotlivých přístupů členských států k ochraně nepominutelných[10] funkcí telekomunikačních sítí.

Samotná ochrana nepominutelných funkcí byla také konzultována se zahraničními organizacemi, úřady majících v gesci problematiku kybernetické bezpečnosti Velké Británie a Německa.

NÚKIB také opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se budoucí regulace, a to především formou obecné výzvy na svých internetových stránkách. Veřejnost tak získala možnost svoje podněty k podobě vyhlášky Úřadu sdělit.

[10] V zahraničí často nesoucí název kritické funkce či kritické komponenty.

B. Zvláštní část

K § 1 – Předmět právní úpravy

Smyslem daného ustanovení je vymezení předmětu regulace navrhované vyhlášky a odkázání na zmocňovací ustanovení Zákona, na základě kterého je podzákonný právní předpis vydáván.

K § 2 – Vymezení pojmů

Pro potřeby vyhlášky je za účelem vymezení oblasti, do které nepominutelné funkce spadají, určena veřejná komunikační síť dle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

Dotčeným ustanovením jsou vymezeny jednotlivé technologie přenosu signálu tak, aby jejich vymezení v Příloze vyhlášky bylo v souladu s termíny užívanými v poli informačních a komunikačních technologií, pro potřeby vyhlášky vycházejících mimo jiné z terminologie obsažené jednak v technických specifikacích 3GPP, konkrétně v technických specifikacích TS 23.501 a TS 23.00, jednak v obdobných úpravách členských států Evropské unie zejména ve Finsku, Velké Británii, Francii a Německu či z Výkladového slovníku kybernetické bezpečnosti, jenž vznikl činností asociace AFCEA a Národního centra kybernetické bezpečnosti Národního bezpečnostního úřadu.

K § 3 – Nepominutelné funkce

Pro potřeby vyhlášky je seznam nepominutelných funkcí obsažen v Příloze vyhlášky, která tyto funkce blíže specifikuje pro jejich identifikaci v jednotlivých architekturách veřejných komunikačních sítí.

K § 4 – Účinnost

Návrh vyhlášky se váže k navrhovanému Zákonu, primárně na ustanovení vztahující se k bezpečnosti dodavatelského řetězce. Z toho důvodu je nezbytné stanovit termín nabytí účinnosti nejpozději k datu uvedenému v návrhu vyhlášky.

K Příloze (Nepominutelné funkce)

Příloha obsahuje seznam specifikující nepominutelné funkce veřejných komunikačních sítí, zejména ve formě softwarových či hardwarových komponent a prvků, jež jsou dle níže popsaných technických specifikací považovány za kritické, tudíž pro účely vyhlášky a bezpečnost dodavatelského řetězce nepominutelné, a to jak pro veřejné komunikační sítě obecně, tak specificky pro 5. a 4. generaci mobilní veřejné komunikační sítě (dále také „5. generace sítí“ a „4. generace sítí“). Uvedené 5. a 4. generace sítí jsou z hlediska prostředí veřejných komunikačních sítí velmi rozšířené a zároveň standardizované na velmi vysoké, sektorem elektronických komunikací uznávané, úrovni kvality. Seznam uvedený v Příloze tudíž sestává jak z univerzálně používaných názvů jednotlivých funkcí, které jsou z důvodu sjednocené praxe v oboru informačních a komunikačních technologií (dále jen „ICT“) uvedeny v anglickém jazyce, včetně rozšířených zavedených zkratek, tak jejich věcnému popisu pro upřesnění úlohy těchto funkcí.

Tyto funkce byly převážně extrahovány z technických specifikací 3GPP TS 23.501 a 3GPP TS 23.002, jejichž kritický význam vyplývá nejen ze samotných technických specifikací, ale i z jejich užití v rámci ochrany kritických částí veřejných komunikačních sítí Spojeného království, Francie, Finska nebo Německa. Jako inspirace pro stanovení nepominutelných funkcí návrhu této vyhlášky posloužily zejména regulace obdobných funkcí ve Finsku, Spojeném království, Francii a Německu.

Příloha návrhu vyhlášky nejprve stanovuje funkce veřejných komunikačních sítí v obecném pojetí tak, aby toto pojetí dopadalo na veškeré sítě veřejných komunikací, včetně 2., 4. či 5. generace sítí a ostatní síťové služby jako je například tzv. IP Multimedia Subsystem, zkráceně IMS dle technických specifikací 3GPP TS 23.228. Smysl takového rozdělení je dvojí. Jednak je určen rozsah, na který se uplatní konkrétní funkce spadající pod 4. a 5. generaci sítí, jak jsou dále popsány v Příloze vyhlášky, jednak takové obecné pojetí představuje vodítko pro určení nepominutelných funkcí, které nelze podřadit pod žádné technologické standardy nebo které jsou méně rozšířené či se nachází ve vývoji.

Ad Nepominutelné funkce ve veřejné komunikační síti

První část Přílohy k vyhlášce definuje síťové funkce ve veřejné komunikační síti, které musí být považovány za kritickou část veřejné komunikační sítě, a tedy pro potřeby vyhlášky za funkce nepominutelné. Seznam je technologicky neutrální z důvodu úpravy funkcí pro jednotlivé technologie a služby fungující napříč veřejnými komunikačními sítěmi. Z hlediska bezpečnosti pro funkce uvedené v první části Přílohy platí, že tyto funkce nemusí být realizovány v plném rozsahu svých možností, ale k jejich zařazení do množiny nepominutelných funkcí ve smyslu vyhlášky postačí částečná realizace těchto funkcí v síťové infrastruktuře. Navíc platí, že jednotlivé softwarové komponenty, síťová zařízení nebo služby mohou jak podporovat část těchto nepominutelných funkcí, tak také více funkcí na jedné komponentě.

Ad číslo 1.1

První funkcionalitou představující nepominutelnou funkci jsou funkce primárně související s řízením síťových zdrojů a směrováním, které mohou mít významný dopad na síťový provoz. Zde náleží kupříkladu služby či komponenty významné co do velikosti zeměpisné oblasti pokrytí, kterou představuje oblast větší nežli 20,000 km^2 nebo počtu připojených uživatelů vyšším nežli 50,000 pro služby SMS, internetu a telefonie, popřípadě 100,000 pro služby tzv. masové komunikace (tj. rozhlasové a televizní vysílání), 200,000 pro e-mailovou komunikaci či 300,000 pro ostatní služby. Uvedené počty jsou spíše orientační, vycházející z dat zahraničních partnerů Úřadu. Nepominutelnost funkce č. 1.1 je závislá na jejím rozhodujícím vlivu pro řízení provozu veřejné komunikační sítě a přístupu pro koncová zařízení uživatelů a jejich mobilitu mezi sítěmi. Řadí se zde také služby nebo komponenty řídící významnou část provozu veřejné komunikační sítě a služby či komponenty datového centra, které jsou nutné pro provoz kritické části veřejné komunikační sítě.

Kromě toho se tato funkce vztahuje na systémy, jež jsou schopné analyzovat uživatelský provoz, a které se používají k odhalování nežádoucího, popř. škodlivého, síťového provozu a které mohou být rovněž zahrnuty do funkcí sloužících k zabezpečení informací. Tyto typy funkcí jsou obvykle implementovány v tzv. jádru sítě, neboli páteřní síti, což je taková část sítě, kterou lze na základě jejího specifického rozhraní oddělit od okrajové části sítě.

V případě mobilních sítí se tento odstavec vztahuje zejména na funkce související s přenosem uživatelské roviny nebo používané k řízení síťového provozu prostřednictvím řídicí roviny, s čímž souvisí řízení mobility v mobilní síti.

Obecně se tyto funkce používají k řízení a správě síťového provozu, a proto je třeba je považovat za kritické části sítě elektronických komunikací, a tedy nepominutelnou funkci veřejné komunikační sítě. Tyto funkce rovněž hrají významnou roli při zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti komunikační sítě jako celku.

Ad číslo 1.2

Toto číslo obsahující zejména evidenci, správu přístupu, ověřování a autorizaci koncových uživatelů představuje klíčovou funkci pro zajištění ověřování uživatelů, přidělování síťových prostředků uživatelům a správu uživatelskou relací za účelem dostupnosti služeb a zachování důvěrnosti komunikace v síti.

Vzhledem k tomu, že do množiny prvků představujících tuto nepominutelnou funkci se rovněž řadí zmíněné ověřování koncových zařízení uživatelů, kontrola a správa přístupů, včetně přidělování síťových prostředků skrz přiřazování IP adres koncovým zařízením a serverů sloužícím uživatelům, z hlediska dostupnosti je tato funkce klíčová.

Skrz přidělování síťových zdrojů musí uvedená funkce komunikovat s řadou dalších síťových funkcí, včetně funkcí nepominutelných, s čímž se pojí také riziko úniku dat v případě kompromitace dané funkce. V neposlední řadě se funkce také významně podílí na řízení síťového provozu, údržbě spojení a zajišťování dostupnosti služeb, důvěrnosti komunikací a informační bezpečnosti komunikační sítě jako celku.

Ad číslo 1.3

Další funkce, tj. registrace, autentizace a autorizace funkcí veřejné komunikační sítě a síťových služeb, patří mezi nepominutelné funkce vzhledem k síťovým registrům užívaným k uchovávání informací o síťových funkcích, jež odpovídají za autorizaci jiných funkcí sloužících mimo jiné k řízení autorizace či účtování zpoplatněných služeb.

Primární účel funkcí čísla 1.3 je kontrola a řízení přístupu síťových funkcí k síti činí z prvků uvedených v písmenu nepominutelnou funkci podílející se na správě přístupu, zajišťování spojení a dostupnosti služeb, včetně napomáhání s důvěrností komunikace a informační bezpečností.

Ad číslo 1.4

Jak je uvedené v Příloze, daná funkce umožňuje přístup k údajům o zeměpisné poloze koncových zařízení zpracovávaných v rámci veřejné komunikační sítě nebo určení polohy zařízení pomocí prostředků veřejné komunikační sítě, čímž pádem odhaluje polohu koncového zařízení, zejména těch s předplacenými službami, tedy i zeměpisnou polohu uživatele za pomoci přijímání geoprostorových dat, včetně provozních a lokalizačních údajů důležitých pro přenos komunikace. Tyto údaje primárně slouží k řízení přístupu k síti, což z funkcí čísla 1.4 činí nepominutelnou funkci co do zajištění přístupu k síti, zejména významného pro případ nouzových situací, kdy je lokalizace uživatelů a zajištění jejich přístupu k síti zcela zásadní.

Ad číslo 1.5

Jedná se o funkce, které slouží převážně k ukládání a načítání síťových, zejména nestrukturovaných dat a dat koncových uživatelů. Ztráta či nemožnost načíst tato data má významný dopad na řízení a správu síťového provozu, převážně pro zajištění dostupnosti služeb uživatelů a zajištění důvěrnosti komunikace a informační bezpečnosti.

Ad číslo 1.6

Uvedené služby představují množinu síťových prvků, služeb a funkcí infrastruktury, které jsou nezbytné pro podporu provozu veřejné komunikační sítě a veřejně dostupné služby elektronických komunikací. Mezi tyto služby se řadí datová úložiště obsahující informace o nepominutelných funkcích veřejné komunikační sítě a údaje o uživatelích, služby přidělování

adres a jmen v jádru sítě, tzv. časové služby sloužící pro synchronizaci času napříč funkcemi (významné pro správu klíčů a protokolů) a centralizovaný systém časových služeb.

Tyto služby jsou zásadní pro zajištění síťového provozu a v důsledky i dostupnost síťových služeb. Jejich role je zásadní pro správu přístupů různých síťových funkcí do veřejné komunikační sítě a synchronizaci síťového provozu, včetně zajištění důvěrnosti komunikace a informační bezpečnosti sítě jako celku.

Ad číslo 1.7

Zavádění rozhraní pro propojování jednotlivých sítí veřejných komunikací či služeb, jako je roaming, se týká zejména vnějších rozhraní jádra sítě, zajišťujících přístup k síťovým službám jiných veřejných komunikačních sítí poskytovaných jedním nebo více operátory. Zde se řadí jak roamingové služby umožňující propojování mezi sítěmi, tak rovněž internetové služby a jejich přístupové brány. Uvedené funkcionality jsou významné pro řízení a správu síťového provozu a přístupu k službám v síti, kvůli čemuž se funkce považuje za důležitou pro zajištění dostupnosti služeb a informační bezpečnost.

Ad číslo 1.8

Množina funkcí upravená číslem 1.8 zahrnuje funkce zpřístupňující jádro sítě třetím stranám, zejména jiným veřejným komunikačním sítím z hlediska bezpečnosti a přístupu. Funkce je vzdor obecnému pojetí považována za nepominutelnou, jelikož slouží jako praktický překladač programových funkcí. Jedná se o přístupovou bránu do jádra sítě, což ji činí zásadní pro zajištění bezpečnost jádra veřejné komunikační sítě.

Ad číslo 1.9

Tato funkce zahrnuje propojovací body zajišťující spojení s jinými veřejnými komunikačními sítěmi a službami umožňujícími přenos provozu mezi uvedenými sítěmi, a to včetně internetového přenosu. Z praktického hlediska množina funkcí čísla 1.9 zahrnuje mimo jiné internetové výměnné body IXP či výměnné body mobilních operátorů DIX, přičemž tyto funkce se používají k řízení a správě síťového provozu, kvůli čemuž musí být považovány za kritické části komunikační sítě. Jejich role pro zajištění provozu sítě, a z toho vyplývající dostupnosti služeb a informační bezpečnosti, je významná.

Ad číslo 1.10

Uvedené funkce zahrnují centralizované funkce sloužící k ukládání, přenosu, zajištění integrity a řízení šifrovacích klíčů uživatelů. V uvedeném případě centralizovanost funkce spočívá v jednotném účelu funkce, což představuje situaci, kdy může být daná funkce rozdělena do několika různých komponent v různých zeměpisných lokacích.

Primární účel funkce čísla 1.10 se vztahuje zejména na oblasti šifrování síťového provozu mezi základnovými stanicemi sítě a jádrem sítě, a to včetně bezdrátových přenosových spojů základnových stanic, šifrování používané komponentami jádra sítě a šifrování funkcí páteřní veřejné komunikační sítě. Zahrnuje rovněž šifrování datových úložišť používaných kritickými částmi komunikační sítě. Dále se písmeno vztahuje nejen na ověřování a šifrování mezi uživateli a sítí, ale také na ověřování a šifrování mezi jednotlivými síťovými prvky a síťovými funkcemi.

Kritickou součástí uvedených funkcí je řízení a správa síťového provozu a přístupu uživatelů k síti, jelikož je významná při zajišťování důvěrnosti komunikace a informační bezpečnosti komunikační sítě jako celku

Ad číslo 1.11

Dané číslo zahrnuje funkce užívané k monitorování, správě či filtrování síťového provozu nebo ke zpracování dat protokolů systémů připojených k dalším nepominutelným funkcím veřejné komunikační sítě. Množina čísla 1.11 se rovněž vztahuje na funkce používané ke správě a monitorování opatření týkajících se údržby nebo správy sítě.

Hlavním smyslem zabezpečení informací je ochrana jádra sítě jak před hrozbami zvnějšku, tzn. ze strany externích veřejných komunikačních sítí, tak rovněž zevnitř ze strany ostatních funkcí sítě. Dále podpora informační bezpečnosti, jako je bezpečnostní software na serverech, umožňuje správu platforem kritických systémů nebo jejich operačních systémů. Odstavec zahrnuje také funkce informační bezpečnosti zaměřené na další kritické části komunikační sítě, jako jsou například ty řídicí spojení. Pro zajištění své funkčnosti může být funkce čísla 1.11 z hlediska architektury sítě implementována i mimo jádro veřejné komunikační sítě, tj. na okrajové síti.

Ad číslo 1.12

Systémy řízení a monitorování veřejné komunikační sítě zpravidla mají významný dopad na přístup k síti a řízení provozu v dané síti. Uvedené systémy řízení a monitorování se vztahují na software a jiná zařízení, která se používají k provozu, údržbě a monitorování zdrojů komunikační sítě, včetně systémů zabezpečení informací, síťových zařízení či obecně softwaru používaného pro síťovou údržbu.

Významný dopad uvedených funkcí spočívá ve skutečnosti, že jsou dané funkce čísla 1.12 schopny umožnit či znemožnit přístup uživatelů či jiných nepominutelných funkcí k síti nebo službám sítě.

Ad číslo 1.13

První složka, tedy funkce fakturační, v angličtině je pro tuto složku užíván pojem invoicing system, uvedená v tomto čísle, souvisí s poskytováním předplatného služeb veřejné komunikační sítě, což může mít významný dopad na přístup k síti v případě kontrolování předplatného jednotlivých uživatelů. Fakturační funkce pro svou povahu často komunikují s dalšími nepominutelnými funkcemi.

Co se týče podpůrných a back-end systémů, například v podobě tzv. Business Support systémů, jsou tyto považovány za nepominutelnou funkci, lze-li předpokládat jejich významný dopad na přístup k veřejné komunikační síti nebo na její provoz, zejména s ohledem na dostupnost služeb. Tyto funkce mohou být přiřazeny jak k jádru sítě, tak také vně.

Ad číslo 1.14

Funkce zavádějící záznam a monitorování provozních a lokalizačních údajů slouží zejména pro zajištění bezproblémového síťového provozu a přístupu k síti. Jejich smyslem je monitorování možných hrozeb a škodlivých událostí v souvislosti s přístupem uživatelů k síti v případě lokalizačních údajů a provozem sítě v případě monitorování provozních údajů. Tyto

funkce jsou nezbytné pro zajištění přístupu a informační bezpečnosti veřejné komunikační sítě. Jejich podstata je totiž monitorovat, identifikovat a zaznamenávat škodlivé údaje.

Ad číslo 1.15

Systémy řízení základnových stanic spravující přístup uživatelů k veřejné komunikační síti se již kvůli schopnosti spravovat přístup uživatelů považují za nepominutelné funkce ve smyslu vyhlášky. V této souvislosti se funkce řízení rádiové přístupové sítě a řízení základnových stanic vztahuje na software a zařízení, která se používají k provozu, údržbě či správě a monitorování základnových stanic 2. generace sítí, tj. veřejných komunikačních sítí využívajících digitálního přenosu rádiového signálu ve standardu GSM, a dále také 4. a 5. generace sítí. Přístup k základnovým stanicím má zcela zásadní vliv na přístup uživatelů k veřejné komunikační síti.

Ad číslo 1.16

Virtualizace sítě je obecně považována za kritickou součást systémů elektronických komunikací, neboť mezi virtualizovanými funkcemi dochází ke sdílení zdrojů, což může z hlediska bezpečnosti informací představovat významné riziko. To je dáno vzájemnou závislostí virtualizovaných funkcí, které se v síti elektronických komunikací neustále ovlivňují například skrz sdílení zdrojů. Přístup k platformě virtualizované funkce má potenciál ohrozit ostatní funkce, z čehož vyplývá, že síťové funkce, které jsou virtualizované na stejné platformě jako jádro sítě, spadají pod tuto nepominutelnou funkci virtualizace sítě. Pokud je tak například centrální jednotka, CU, virtualizovaná na stejné platformě jako jádro sítě, bude i tato spadat pod nepominutelné funkce čísla 1.16.

Ad Nepominutelné funkce sítí 4. generace

Tato část přílohy definuje funkce sítě, které jsou považovány za nepominutelné funkce mobilní veřejné komunikační sítě 4. generace, tedy tzv. 4G mobilní sítě, s odkazem na síťové funkce popsány technickými specifikacemi TS 23.002 organizace 3GPP. Ne všechny funkce, na něž zmíněné technické specifikace odkazují, především v rámci bodů 4.1.1, 4.1.4 či 4.1.5 těchto specifikací, mohou být považovány za nepominutelné. Z toho důvodu jsou v tabulce Přílohy umístěny pouze takové funkce, které jsou technickými specifikacemi považovány za kritické části komunikační sítě tak, jak je chápe 3GPP.

Seznam nepominutelných funkcí pro 4. generaci sítí, jak je uveden v tabulce Přílohy, není vyčerpávající, a správce sítě či povinná osoba má posoudit, zda v jejich síti existují kromě funkcí uvedených v tabulce i další kritické funkce, které lze určit spojením funkcí 4. nebo 5. generace sítí s definicí veškerých funkcí veřejné komunikační sítě, jak je uvedeno v první části přílohy.

Funkce 4. generace sítí uvedené v příloze obsahují logický výčet, kdy by každá uvedená funkce měla být považována za nepominutelnou funkci dle technických specifikací 3GPP i v případě, kdy komponenta implementují jen část uvedené funkce, nikoliv celý rozsah funkce, která je Přílohou určena jako nepominutelná. Zároveň platí, že softwarové komponenty mohou podporovat více než jednu funkci uvedenou v tabulce.

Nutno dodat, že kromě technologií LTE, určené konkrétně 3GPP LTE (Release 8 a vyšší) nebo IEEE 802.16m, či LTE Advanced, se uvedený seznam nepominutelných funkcí pro 4. generaci vztahuje i na tzv. režim 5G NSA, tedy tzv. non stand-alone mód 5. generace sítí. Tento režim označuje situaci, kdy funkce sítě 5. generace pracují na infrastruktuře sítě 4. generace. Seznam funkcí v Příloze je také ve shodě s analogickými seznamy kritických funkcí

sítí elektronické komunikace ve Spojeném království, Francii a Finsku, které jsou blíže představeny v obecné části této důvodové zprávy.

Ad číslo 2.1

První funkce seznamu představuje centrální databázi, která obsahuje údaje pro zpracování uživatelských relací a jejich připojení k síti elektronické komunikace založené na technologii LTE. Tato funkce převážně zpracovává správu přístupu uživatelů, jejich identifikaci, profilaci a mobilitu. Mimo to je funkce odpovědná za správu klíčů a vytváření ochranných vektorů pro ověřování uživatelů, s čímž souvisí i její další funkcionalita, kterou je provádění tzv. odposlechu a sledování komunikace skrz tzv. Lawful Interception, dále též LI. Dle technických specifikací funkce č. 2.1 zahrnuje další funkce, jako je tzv. Home Location Register či Authentication Centre.

Zmíněné ukládání dat pro zpracování uživatelských relací slouží i ke kontrole a správě přístupu uživatelů k síti, což souvisí s řízením sítě elektronických komunikací, konkrétně s řízením provozu uvnitř této sítě, údržbou spojení a zajišťováním dostupnosti komunikačních služeb. Tato funkce významně ovlivňuje důvěrnost síťové komunikace a informační bezpečnost sítě elektronických komunikací, pročež musí být tato funkce považována za nepominutelnou.

Ad číslo 2.2

Uvedená funkce PGW představuje tzv. síťovou bránu pro paketová data, tzn., že PGW funguje jako rozhraní mezi sítí LTE a dalšími sítěmi, přičemž pracuje s tzv. paketovými daty, užívanými ve službách typu internet nebo sítě IMS založené na protokolu SIP. Tato funkce zahrnuje další služby, zejména správu kvality služeb, tzv. Quality of Service, zkráceně QoS, či hloubkovou kontrolu paketů.

Funkce je považována za nepominutelnou vzhledem k její klíčové roli pro integraci velkého množství funkcí jádrové sítě, zajištění dostupnosti dat či možnosti detekce, blokování nebo zachycení síťového provozu.

Ad číslo 2.3

Tato brána přepojující pakety mezi vnitřní IP sítí operátora a externí IP sítí je funkcí, jež také zaštiťuje přidělování IP adres koncovým zařízením, vynucování zásad používání sítě či filtrování a analýzu provozu, což souvisí s umožněním účtovat poplatky a řídit provoz sítě elektronických komunikací.

Vzhledem k tomu, že se funkce PDN-GW čísla 2.3 považuje za součást řízení a správy síťového provozu, je tato funkce taktéž považována za kritickou, a tedy nepominutelnou součást sítě elektronických komunikací. Uvedená funkce má zásadní roli při zajišťování dostupnosti služeb a důvěrnosti komunikace v síti.

Ad číslo 2.4

Daná funkce ePDG jednak vytváří přístup k jinému, nežli 3GPP směrování provozu, zejména mezi funkcí PDN-GW a uživatelem, jednak implementuje služby VoWiFi, tedy služby bezdrátového volání přes tzv. místní síť Voice over Wi-Fi. Funke ePDG také aktivuje výměnu klíčů mezi uživatelem k vytvoření bezpečného komunikačního tunelu, včetně ověřování a autorizace v rámci tohoto tunelu s implementací funkce LI.

Jelikož tato funkce řídí a spravuje síťový provoz, je považována za kritickou, tedy nepominutelnou funkcí sítě elektronických komunikací. Funkce zajišťuje dostupnost služeb, převážně skrz udržování spojení mezi uživateli, a důvěrnost komunikace v síti.

Ad číslo 2.5

Uvedená funkce PCRF zajišťuje, aby provoz v síti na uživatelské úrovni odpovídal profilům jednotlivých uživatelů ve veřejné komunikační síti. Funkce svou povahou zajišťuje kvalitu služeb připojení uživatelů a implementuje zpoplatnění hlasových služeb VoLTE či tzv. roamingu. Jelikož funkce slouží k řízení a správě síťového provozu, primárně pak k přístupu uživatelů k síti, je tato považována za nepominutelnou pro potřeby veřejných komunikačních sítí. PCRF významně napomáhá k zajišťování dostupnosti služeb v podobě údržby a řízení spojení.

Ad číslo 2.6

Daná funkce mimo jiné umožňuje ukončení provozu na řídící úrovni koncových zařízení, registraci koncových zařízení a správu koncového připojení a mobility, což se váže i na služby roamingu. Vzhledem k řízení a správě přístupů uživatelů k síti elektronických komunikací je potřeba funkci považovat za nepominutelnou z hlediska bezpečnosti dodavatelského řetězce. Funkce se podílí na řízení a provozu sítě elektronických komunikací, dostupnosti spojení a služeb, důvěrnosti komunikace a informační bezpečnosti sítě elektronických komunikací jako celku.

Ad číslo 2.7

Brána MME odpovědná za směrování provozu na uživatelské úrovni obstarává směrování provozu mezi základnovými stanicemi a funkcí PDN-GW. Funkce MME dále vytváří nová spojení a upravuje stávající spojení mezi koncovými zařízeními a sítí elektronických komunikací, přičemž z hlediska ochrany síťového provozu implementuje funkce LI. Primární účel MME, tedy řídit a spravovat síťový provoz, řadí tuto funkci mezi nepominutelné funkce. MME je klíčová pro zajištění spojení a dostupnosti služeb a důvěrnosti komunikace v síti elektronických komunikací.

Ad číslo 2.8

Funkce SLF předává název centrální databáze dalším nepominutelným funkcím, jako je AAA. Uvedené slouží k řízení a správě přístupů uživatelů k síťovým službám, což staví funkci SLF do role nepominutelné funkce z hlediska kontroly, řízení sítě elektronických komunikací a jejího provozu, dostupnosti spojení a služeb, důvěrnosti komunikace a bezpečnosti informací.

Ad číslo 2.9

Registr identit EIR představuje databázi veřejné komunikační sítě sloužící primárně k registru totožnosti jednotlivých zařízení. EIR zejména uchovává mezinárodní identifikační čísla mobilních zařízení a informuje ohledně oprávnění užívat jednotlivá mobilní zařízení v síti. EIR zároveň spravuje tzv. černou listinu, která znemožňuje přístup všech koncových zařízení a adres k síti elektronických komunikací.

Z výše uvedeného vyplývá funkcionalita EIR jakožto kontrolora přístupu uživatelů k síti, což řadí EIR mezi nepominutelné funkce sítě elektronických komunikací. Funkce také slouží k zabránění používání neoprávněných zařízení v síti, k zajištění dostupnosti síťových služeb a informační bezpečnosti.

Ad číslo 2.10

3GPP AAA Server kromě zajištění autorizace také spravuje mobilitu uživatelů s přístupem mimo 3GPP a ukládá údaje o uživatelích za účelem správy přístupu, jenž jsou potřebné převážně ke správě přístupu do sítě. Další funkcionalitou 3GPP AAA serveru je také implementace služby VoWiFi a funkce LI. Z důvodu řízení přístupu uživatelů k síti se považuje tato funkce za nepominutelnou funkci sítě elektronických komunikací. Představuje významnou roli pro zajištění důvěrnosti komunikace, kontrolu, správu, provoz, a tím pádem i dostupnost sítě jako celku.

Ad číslo 2.11

Proxy server odpovědný za ověřování a autorizaci uživatelů s přístupem mimo 3GPP oproti předchozímu 3GPP AAA serveru poskytuje odpovídající služby jako 3GPP AAA, ale pro služby roamingu. Dále zmíněný Proxy AAA server vybírá bránu pro relace uživatele pro roaming. Z toho vyplývá významná role uvedené funkce pro zajištění přístupu uživatelů k síti, která určuje Proxy AAA Server jako nepominutelnou funkci sítě elektronických komunikací.

Ad číslo 2.12

Funkce řídící uživatelský provoz mezi mobilní sítí a přístupovými sítěmi mimo 3GPP se týká sítí jako je WLAN a sdílí data za účelem směrování provozu a mobility koncových zařízení v síti, což slouží k řízení a správě síťového provozu uživatelů. Funkce také významně přispívá k zajištění dostupnosti sítě a služeb, a je tudíž považována ze nepominutelnou pro sítě elektronických komunikací.

Ad Nepominutelné funkce sítí 5. generace

V pořadí třetí část přílohy určuje funkce 5. generace mobilní veřejné komunikační sítě, jež lze považovat za nepominutelné z hlediska jejich kritičnosti popsané převážně v technických specifikacích 3GPP TS 23.501. Funkce určené ve zmíněných specifikacích jsou standardizované, dobře popsané a často rozdělené mezi vícero aplikací či komponent. Výčet extrahovaných kritických funkcí pro 5. generaci sítí je uveden v tabulce Přílohy.

Každá funkce z této části přílohy by měla být považována za nepominutelnou funkci také v případě, kdy jednotlivá komponenta podporují pouze část uvedené funkce, která je určená jako nepominutelná.

Pro potřeby vyhlášky je 5. generace sítí chápána jako veřejné komunikační sítě vyhovující standardu sítí elektronických komunikací dle specifikace 3GPP/ETSI, zahrnující minimálně standard přístupové rádiové sítě 5G NR (New Radio) v architektuře, která splňuje požadavky specifikací ETSI TS 123 501 (3GPP TS 23.501) a ETSI TS 138 401 (3GPP TS 38.401) nebo aktuálnějších.

Ad číslo 3.1

Funkce AUSF spravuje funkce spojené s ověřováním koncových zařízení uživatelů a zároveň poskytuje jednotný rámec pro ověřování připojení. Primární funkcionalitou AUSF je správa síťového provozu a přístup uživatelů k síti, kvůli čemuž je funkce považována za nepominutelnou. Její další role je uplatňována při zajišťování dostupnosti sítě, služeb, zaručení důvěrnosti komunikace a informační bezpečnost sítí elektronické komunikace.

Ad číslo 3.2

Funkce AMF kromě účelu popsaném v Příloze vyhlášky slouží k připojení základnových stanic a koncových zařízení rádiové sítě a jejich registrace k jádru sítě, jakož i samotné správě mobility. Dále AMF vytváří, spravuje a obstarává přesah přístupu koncových uživatelů k sítím mimo mobilní síť, jako např. k WLAN. K AMF se rovněž váže možnost tzv. odposlechu síťového provozu a sledování komunikace skrz funkci LI.

Role AMF při kontrole a správě přístupu uživatelů k síti znamená určení AMF jako nepominutelné funkce, která má významnou roli pro řízení síťového provozu, udržování spojení, zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnost sítě elektronických komunikací jako celku.

Ad číslo 3.3

Funkce Unstructured Data Storage Function, zkráceně také UDSF, bývá zpravidla využívána ostatními funkcemi k ukládání a načítání nestrukturovaných dat, která se vážou k údajům ohledně připojení, stavu jednotlivých funkcí, včetně těch nepominutelných, či obecně relacím v síti. V případě jejího využití funkce UDSF přispívá k řízení a správě síťového provozu, čímž musí být považována za nepominutelnou funkci sítě elektronických komunikací. Účel její implementace přispívá k zajištění dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti sítě elektronických komunikací.

Ad číslo 3.4

Funkce umožňující poskytování funkcí jádra 5G sítě třetím stranám a externím aplikacím mimo jiné umožňuje i bezpečnou komunikaci jiných funkcí se sítí a ukládání dat těchto funkcí. Jako nepominutelná je tato funkce považována z důvodu řízení přístupu uživatelů k funkcím sítě, což je klíčové pro důvěrnost komunikace, přístupu k službám a informační bezpečnost sítě.

Ad číslo 3.5

Daná funkce, umožňující poskytování funkcí jádra 5. generace sítě třetím stranám a externím aplikacím, funguje téměř totožně jako funkce NEF s tím rozdílem, že je tato funkce užívána pro roaming. Z toho důvodu je považována za nepominutelnou.

Ad číslo 3.6

Funkce NRF spravuje seznam síťových služeb a komponent, čímž obstarává registraci služeb a vyhledávání funkcí. Usnadňuje tak vzájemnou dostupnost či komunikaci jednotlivých funkcí a služeb v síti. Jelikož všechny funkce sítě 5. generace komunikují s NRF, její význam je naprosto stěžejní pro předávání informací, čímž se řadí do seznamu nepominutelných funkcí. Její role je zásadní pro dostupnost sítě a služeb a informační bezpečnost sítě.

Ad číslo 3.7

Funkce NSSF slouží mimo jiné ke kontrole a výběru povolených nebo obecně koncových zařízení sítě. Funkce spravuje síťový provoz a přístup uživatelů k síti, což z ní dělá nepominutelnou funkci pro zajištění dostupnosti sítí, služeb, důvěrnosti komunikace a informační bezpečnost sítě.

Ad číslo 3.8

Funkce NSSAAF slouží ke kontrole a správě přístupů uživatelů k síti elektronických komunikací, což je významné pro zajištění dostupnosti služeb, důvěrnosti komunikace a dat a informační bezpečnosti sítě. Uvedené NSSAAF řadí mezi nepominutelné funkce.

Ad číslo 3.9

Tato funkce PCF je odpovědná za řízení provozu a zavedení politiky přístupu, tedy zásad řízení přístupu, kdy zmíněná funkce představuje zásadní prvek pro řízení kvality služeb a zpoplatňování služeb v síti elektronických komunikací. PCF tak určuje politiky podporující rozdělení sítě, politiky mobility a roamingu. Uvedené skutečnosti z ní činí jednotku podílející se na řízení i správě síťového provozu a přístupů uživatelů k síti a řadí ji tak mezi nepominutelné funkce veřejné komunikační sítě, kdy je PCF obzvlášť významná pro zajištění dostupnosti služeb sítě.

Ad číslo 3.10

Funkce řídící uživatelské relace, zkráceně SMF, kombinuje a spravuje více funkcí řízení provozu správy relací dle síťových protokolů, přiděluje IP adresy a rovněž implementuje funkci LI. Její role je významná v řízení a správě síťového provozu. Ze zmíněného a z důvodu zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti veřejné komunikační sítě se funkce řadí mezi nepominutelné funkce.

Ad číslo 3.11

Funkce UDM mimo funkcionality zmíněné v Příloze odpovídá za identifikaci a registr uživatelů, správu předplatného a vytváření a správy šifrovacích klíčů. UDM dále definuje či odstraňuje účastníky ve veřejné komunikační síti 5. generace, monitoruje výměnu karet SIM, změnu čísel MSISDN nebo upravuje údaje o objednávkách. Protože funkce vykonává další práci obdobnou funkci HSS a implementuje funkci LI, její role při řízení a kontrole uživatelů k síťovým službám ji činí nepominutelnou.

Ad číslo 3.12

Datové úložiště UDR představuje významnou funkci pro ukládání a načítání dat, včetně strukturálních a aplikačních dat z nepominutelné funkce NEF. Úlohou UDR je řídit a spravovat síťový provoz a zajistit tak dostupnost služeb, důvěrnost komunikace a informační bezpečnost sítě. To z UDR činí nepominutelnou funkci sítí elektronických komunikací.

Ad číslo 3.13

Funkce UPF je primárně odpovědná za řízení kvality služeb, filtrování a šifrování provozu na uživatelské rovině nebo udržování kontinuity relací a síťových služeb. Funkce tedy slouží k řízení a správě síťového provozu uživatelů a tudíž se řadí mezi nepominutelné funkce obstarávající dostupnost spojení a důvěrnost komunikace.

Ad číslo 3.14

Funkce pro ukládání a uchovávání identifikačních dat uživatelských zařízení mimo zmíněné ukládá údaje o rádiových schopnostech koncových zařízení, což zahrnuje informace o podporovaných rádiových technologiích či kmitočtových pásmech, jakož další schopnosti

rádiové sítě. Ze své podstaty funkce zajišťuje kontrolu a řídí přístup k sítí, což z ní činí nepominutelnou funkci podílející se na zajištění dostupnosti služeb.

Ad číslo 3.15

Funkce AF především určuje směrování na základě aplikací uživatelů a skrz nepominutelnou funkci NEF také komunikaci s jádrem sítě. Primárně má tato funkce za cíl řídit a spravovat síťový provoz, konkrétně přístup k síti natolik významným způsobem, že je tato funkce považována za nepominutelnou co do zajištění dostupnosti služeb a z toho vyplývající informační bezpečnosti sítě.

Ad číslo 3.16

Registr identit zařízení a vybavení 5G-EIR vytváří tzv. černou listinu, jež znemožňuje přístup nepovoleným zařízením k veřejné komunikační síti. Účel funkce spočívající v kontrole a řízení přístupu uživatelů do sítě na základě uvedené černé listiny řadí 5G-EIR mezi nepominutelné funkce. Této funkce lze přisuzovat zásadní roli v zajištění dostupnosti služeb z důvodu řízení přístupu.

Ad číslo 3.17

Funkce NWDAF shromažďující a analyzující data pro řízení sítě využívá strojové učení, tzv. machine learning, ke shromažďování dat a poskytování těchto dat ostatním funkcím v reálném čase. K dalším, neméně podstatným, funkcionalitám NWDAF se řadí provádění prediktivních analýz a proaktivní správa 5. generace sítí. NWDAF představuje komplexní funkci, která rovněž slouží k automatizovanému škálování síťové infrastruktury, přiřazování síťových úseků, správě přístupů do těchto úseků a zajištění mobility v síti.

Vzhledem k rozšíření NWDAF musí být naplněna složka podstatného řízení provozu v síti, to znamená, že v případě distribuované implementace s jednou či nižšími jednotkami NWDAF je tato funkce považována za nepominutelnou vždy, jelikož v těchto případech významně řídí a spravuje síťový provoz. NWDAF představuje obzvlášť významný nástroj pro dostupnost služeb.

Ad číslo 3.18

Funkce umožňující online a offline platby CHF představuje funkci významnou pro způsoby účtování za služby poskytované v rámci využívání sítě elektronických komunikací. Funkce CHF komunikuje s ostatními funkcemi 5. generace sítí a podporuje zpracování informací o účtování uživatelů, dále také generuje tzv. tikety, tedy systémové požadavky vyřešit problém, směruje síťový tok zpráv o účtování a monitoruje poruchy či výpadky související s účtováním. Význam funkce tkví v monitorovacích schopnostech funkce a zajištění důvěrnosti komunikace mezi funkcemi, což z CHF činí nepominutelnou funkci.

Ad číslo 3.19

Funkce směrování zpráv do ostatních síťových funkcí SCP kromě směrování a přenášení zpráv mezi funkcemi zjednodušuje topologii veřejné komunikační sítě, vyrovnává zátěž sítě či možné přetížení co do množství zpráv za účelem integrace v prostředí s větším množstvím komponent. Z tohoto důvodu je funkce považována za nepominutelnou, pakliže skrz řízení přenášení zpráv obstarává významnou roli při zajišťování dostupnosti služeb, důvěrnosti komunikace a informační bezpečnosti.

Ad číslo 3.20

Proxy server SEPP podporuje skrytí topologie sítě a zavádí filtrování zpráv, včetně jejich monitorování, na rozhraní řídící i uživatelské roviny mezi mobilními sítěmi. To ve své podstatě znamená také zajištění přístupu do jiných sítí v případě užívání služeb roamingu a obecně podílení se na řízení a správě síťového provozu, pročež je funkce považována za nepominutelnou.

Ad číslo 3.21

Funkce N3IWF kromě uvedeného v Příloze také umožňuje přístup k jádru 5. generace veřejné komunikační sítě prostřednictvím bezdrátové místní sítě WLAN. Tato funkce také podporuje vytvoření zabezpečeného komunikačního tunelu s koncovými zařízeními a autorizuje přístup uživatelů k jádru sítě 5G. Jelikož tímto zajišťuje dostupnost služeb, obstarává důvěrnost komunikace a v důsledku také informační bezpečnost celé sítě, její role je nepominutelná.

Ad číslo 3.22

Funkce TNGF představuje součást přístupové sítě tzv. Trusted Non-3GPP Access Network. Její účel spočívá v zajištění postupného propojení uživatele s jádrem sítě. V praktickém užití je funkce TNGF analogií N3IWF, ovšem vyjma možnosti použití šifrovaného tunelu. Z toho důvodu se, tak jako N3IWF, řadí mezi nepominutelné funkce sítě elektronické komunikace.

Ad číslo 3.23

Funkce propojení W-AGF zajišťuje zpřístupnění sítě 5. generace sítí koncovým zařízením uživatelů. Význam funkce spočívá také v konvergenci bezdrátového a drátového připojení s jednotným zajištěním bezpečnostně přístupových postupů, jakož i zajištění kvality služeb či podpory řízení provozu. Funkce je tak zařazena na seznam nepominutelných funkcí.